Claims

1.-6. (canceled)

7. (new) A method for operating a communication terminal for packet-oriented data transmission, the method comprising:

storing a status information for a communication terminal in a memory unit associated with the communication terminal;

providing the status information with a digital signature calculated from the status information by a private key for an asymmetrical encoding method, wherein the private key is associated with a first control unit associated with the communication terminal for the resolution and/or conversion of network addresses;

transmitting a request to associate the communication terminal with at least one second control unit if the first control unit fails, the request comprising the status information and the digital signature;

checking the digital signature; and

associating the communication terminal with the second control unit in the event of a positive check result.

8. (new) The method according to claim 7, wherein the status information is updated at least at a predefinable time upon the initiation of the first or second control unit.

9. (new) The method according to claim 7, wherein the digital signature is calculated from a hash value acquired for the status information.

10. (new) The method according to claim 8, wherein the digital signature is calculated from a hash value acquired for the status information.

11. (new) The method according to claim 7, wherein a hash value is calculated for the status information for the purposes of checking the digital signature and said hash value is compared for a match with a digital signature decoded by using a public key associated with the first control unit.

12. (new) The method according to claim 8, wherein a hash value is calculated for the status information for the purposes of checking the digital signature and said hash value is compared for a match with a digital signature decoded by using a public key associated with the first control unit.

13. (new) The method according to claim 9, wherein the hash value is calculated for the status information for the purposes of checking the digital signature, and wherein the hash value is compared for a match with a digital signature decoded by using a public key associated with the first control unit.

14. (new) The method according to claim 10, wherein the hash value is calculated for the status information for the purposes of checking the digital signature, and wherein the hash value is compared for a match with a digital signature decoded by using a public key associated with the first control unit.

15. (new) The method according to claim 9, wherein a message digest no. 5 algorithm is used for calculating the digital signature.

16. (new) The method according to claim 10, wherein a message digest no. 5 algorithm is used for calculating the digital signature.

17. (new) The method according to claim 11, wherein a message digest no. 5 algorithm is used for calculating the digital signature.

18. (new) The method according to claim 12, wherein a message digest no. 5 algorithm is used for calculating the digital signature.

19. (new) The method according to claim 13, wherein a message digest no. 5 algorithm is used for calculating the digital signature.

20. (new) The method according to claim 14, wherein a message digest no. 5 algorithm is used for calculating the digital signature.

21. (new) A method for operating a communication terminal for packet-oriented data transmission, comprising:

storing at least one piece of status information for a communication terminal in a memory unit associated with the communication terminal, wherein

said status information is provided with a digital signature that is calculated from the status information by means of a private key for an asymmetrical encoding method associated with a first control unit associated with the communication terminal for the resolution and/or conversion of network addresses, wherein,

if the first control unit fails, a request is transmitted comprising the status information and the digital signature to associate the communication terminal with at least one second control unit and the digital signature is checked, and wherein

in the event of a positive check result, the communication terminal is associated with the second control unit.

22. (new) The method according to claim 21, wherein the one piece of status information at least is updated at a predefinable time upon the initiation of the first or second control unit.

23. (new) The method according to claim 21, wherein the digital signature is calculated from a hash value ascertained for the status information.

24. (new) The method according to claim 23, wherein a hash value is calculated for the status information for the purposes of checking the digital signature and said hash value is compared for a match with a digital signature decoded by using a public key associated with the first control unit.

25. (new) The method according to claim 23, wherein a message digest no. 5 algorithm is used for calculating the digital signature.

26. (new) A control program for operating a communication terminal for packet-oriented data transmission, which can be loaded into a working memory of a computing facility and displays at least one block of code, in the execution of which

at least one piece of status information is stored, for a communication terminal, in a memory unit associated with the communication terminal,

said status information is provided with a digital signature that is calculated from the status information by means of a private key for an asymmetrical encoding method associated with a first control unit associated with the communication terminal for the resolution and/or conversion of network addresses,

if the first control unit fails, a request is transmitted comprising the status information and the digital signature to associate the communication terminal with at least one second control unit and a check of the digital signature is initiated,

in the event of a positive check result, the association of the communication terminal with the second control unit is initiated,

if the control program is running on the computing facility.